Large caps in projective Galois spaces

Jürgen Bierbrauer* Yves Edel†

Key Words: Caps, Galois geometries, codes.

AMS Subject Classification: 51E22, 94B05.

1 What is a cap?

A **cap** in a projective or affine geometry over a finite field is a set of points no three of which are collinear. The most natural question to ask is:

```
What is the maximum size of a cap in the given space?
```

This is also known as the **packing problem.** In this paper, $m_2(r,q)$ denotes the size of the largest caps in $\mathrm{PG}(r,q)$.

2 Classical examples

If the underlying field is $\mathbb{F}_2$, the answer is easy: $\mathrm{AG}(n,2)$ is itself a cap of 2^n points and it forms up to projective equivalence the unique largest cap in $\mathrm{PG}(n,2)$.

Assume therefore we work in $\mathrm{PG}(n,q)$ or $\mathrm{AG}(n,q)$ for $q>2$. The canonical models for caps are quadrics of Witt index 1. They yield $(q+1)$-caps in $\mathrm{AG}(2,q)$ (and in $\mathrm{PG}(2,q)$) and obviously these **ovals** are maximal for odd q. In odd characteristic each oval in $\mathrm{PG}(2,q)$ is a conic section (Segre [49,50]). This is not true in characteristic 2, where moreover each oval O is embedded in a unique **hyperoval** $O\cup\{N\}$. Here N is the **nucleus**, the intersection of all the tangents to O. A hyperoval is a $(q+2)$-cap and this is maximal. The hyperovals are described by a special kind of permutation polynomials. This is an active line of research, see the survey [38]. In $\mathrm{PG}(3,q)$ an elliptic quadric is a (q^2+1)-cap. This is maximal for all $q>2$ (see Bose [13] and Qvist [47]). Its affine part is a q^2-cap in $\mathrm{AG}(3,q)$ and this is maximal. In characteristic 2 the Tits ovoids form another family of (q^2+1)-caps in $\mathrm{PG}(3,q)$, see [55]. They may be considered classical as they admit a family of classical groups, the Suzuki groups ${}^2B_2(q)$ for $q=2^{2m+1}$, as groups of automorphisms.

*Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA. E-mail address: jbierbra@mtu.edu

†Ghent University, Department of Mathematics, Krijgslaan 281 S22, B–9000 Gent, Belgium. E-mail address: yedel@cage.ugent.be. The research of this author takes place within the project "Linear codes and cryptography" of the Research Foundation – Flanders (FWO) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme - Belgian State - Belgian Science Policy: project P6/26-Bcrypt.

3 Exceptional caps

For projective dimensions $d > 3$ and fields $\mathbb{F}_q, q > 2$, the basic question seems to be hard to answer. Only for some small dimensions and fields the answer is known. In those cases, the corresponding maximal caps tend to be exotic, in particular more or less uniquely determined and very symmetric.

The ternary case

In $\mathrm{PG}(4,3)$ and $\mathrm{AG}(4,3)$, the maximum is 20 (see Pellegrino [45]), with the 20-cap in $\mathrm{AG}(4,3)$ (the **Pellegrino cap**) uniquely determined. In $\mathrm{PG}(5,3)$ and $\mathrm{AG}(5,3)$, the maximum is 56 and 45 respectively. In both cases, the caps are uniquely determined, the **Hill cap** in $\mathrm{PG}(5,3)$ and the **affine Hill cap** (contained in the Hill cap) in $\mathrm{AG}(5,3)$. The unicity was shown by Hill [36] in the projective, in [6, 25] in the affine case. The automorphism group of the Hill cap is an extension of the simple group $\mathrm{PSL}(3,4)$ by a group of order 2. There are numerous links to other exceptional mathematical structures, see Hill [37]. The points of the elliptic quadric in $\mathrm{PG}(5,3)$ can be chosen to be the one-dimensional subspaces of $\mathbb{F}_3^6$ generated by the vectors of weights 3 or 6. This indicates how those 112 points can be split into two halves each of which forms a cap (for details, see [6]). The automorphism group of the Hill cap is a rank 3 permutation group on the points of the Hill cap, the stabilizer of a point having orbits of lengths $1, 10, 45$. The points of the long orbit form a copy of the affine Hill cap whose automorphism group is the stabilizer $\mathrm{PGL}(2,9)$. The remaining 11 points form a block of the uniquely determined $(56, 11, 2)$-symmetric design (a biplane).

There is a general doubling construction, see [42].

Theorem 1. *An n-cap in $\mathrm{PG}(d,q)$ allows the construction of a $2n$-cap in $\mathrm{AG}(d+1,q)$.*

This also explains the Pellegrino cap in $\mathrm{AG}(4,3)$. It follows from the doubling construction applied to the elliptic quadric in $\mathrm{PG}(3,3)$. When applied to the Hill cap, doubling yields a 112-cap in $\mathrm{AG}(6,3)$. Potechin [46] showed that this cap is maximal and uniquely determined. Starting from $\mathrm{PG}(6,3)$ we are in uncharted territory. Most of the known constructions of large caps in higher dimensional spaces over $\mathbb{F}_3$ make use of the Hill cap. This starts with the Calderbank-Fishburn 236-cap [14] in $\mathrm{AG}(7,3)$ and a 248-cap in $\mathrm{PG}(7,3)$ (see [21]). Those caps have as automorphism groups semidirect products of E_{32} by S_5 and of E_{64} by S_5, respectively. Exceptions are a recently discovered 541-cap in $\mathrm{PG}(8,3)$ and a 2744-cap in $\mathrm{PG}(10,3)$ which resulted from a computer search. The game of SET can be used as a playful motivation to study caps in affine ternary spaces, see [7, Section 3.6] and [16]. The 81 cards of the game correspond to the points of $\mathrm{AG}(4,3)$ and a cap is a point set not containing a SET. Thanks to Pellegrino, Hill, and Potechin, we now know what are the largest cardinalities of SET-free collections of cards in the d-dimensional generalizations of the game where $d \leq 6$.

When $q > 3$

The maximum sizes of caps in $\mathrm{PG}(4,4)$ and $\mathrm{AG}(4,4)$ are 41 and 40, respectively. The 40-cap in $\mathrm{AG}(4,4)$ is uniquely determined [22]. It is complete in $\mathrm{PG}(4,4)$. Its automorphism group is a semidirect product of E_{16} and A_5. It can be shown that the two 41-caps given

in [19] are in fact the only 41-caps in PG$(4,4)$. There is a relation of duality between one of the two 41-caps in PG$(4,4)$ and the 40-cap K in AG$(4,4)$: embed AG$(4,4)$ in PG$(4,4)$. There are 40 hyperplanes of PG$(4,4)$ meeting K in 4 points. Those hyperplanes together with the empty hyperplane form the dual of a 41-cap. The other 41-cap in PG$(4,4)$ had in fact been found earlier, by Tallini [54]. Its automorphism group is solvable of order 240. Hill [36] observes: *For each of the known values of $m_2(r,q)$, there is a cap K in* PG(r,q) *of that size on which* Aut(K) *acts as a transitive permutation group.* Unfortunately, this is no longer true as none of the two 41-caps in PG$(4,4)$ admits a transitive automorphism group. Still the metarule that extremal objects tend to be very symmetric is verified also here: the more symmetric 41-cap has a large automorphism group which is transitive on all but one of its points.

Another exceptional object is the Glynn cap [33], a 126-cap in PG$(5,4)$. It contains a 120-cap in AG$(5,4)$ and admits PGL$(3,4)$ as an automorphism group. Observe that this is the second time we encounter the simple group PSL$(3,4)$. We saw it acting on the ternary Hill cap as well.

4 The link to linear codes

Let K an n-cap in PG$(k-1,q)$ and G a $k\times n$ matrix whose columns are representatives of the points of K. Then G is a check-matrix of a $[n,n-k,4]_q$-code $C^\perp$ and this is an equivalent description of the cap property. Its dual $C=C(K)$ may be called a cap-code. It is a projective $[n,k,d]_q$-code where d is the largest number such that outside every hyperplane H of PG$(k-1,q)$ there are at least d points of K. Good caps often yield good cap-codes as well. For example, Pellegrino's result implies directly that the code of the Hill cap is an $[56,6,36]_3$-code and this is a code meeting the Griesmer bound with equality (see [7, Theorem 5.7]).

5 General bounds

The best known general upper bound on the size of a cap uses a version of the Fourier transform (see [10], Meshulam [41] and [7, Section 16.3]). Let $C_k(q)$ be the maximum size of a cap in AG(k,q) and $c_k(q)=C_k(q)/q^k$. Then

$$c_k(q)\le (q^{-k}+c_{k-1}(q))/(1+c_{k-1}(q)) \text{ for } q>2, k\ge 3.$$

A weak form states

$$c_k(q)\le (k+1)/k^2 \text{ for } q>2, k\ge 3.$$

Together with the doubling construction (Theorem 1) this also yields bounds on caps in projective spaces. In fact, if there is an n-cap in PG$(k-1,q)$ then there is a $2n$-cap in AG(k,q), hence $n\le C_k(q)/2$. In low dimensions, the bounds of [53] are better.

6 Recursive constructions

The archetype of all recursive cap constructions is Mukhopadhyay's product construction from [42]. Here is a generalization, [7, Theorem 16.62]:

Theorem 2. *If there is an n-cap $K_1 \subset AG(k,q)$ and an m-cap $K_2 \subset PG(l,q)$, then there is a cap (the product cap) of nm points in* $\mathrm{PG}(k+l,q)$.

If A is avoided by $i \geq 1$ hyperplanes in general position and B by $j \geq 0$ hyperplanes in general position, then the product cap is avoided by $i+j-1$ hyperplanes in general position.

The doubling construction Theorem 1 is a special case of Theorem 2. Here is a generalization, [7, Theorem 16.63]:

Theorem 3. *Assume the following exist:*

- *An n-cap in* $\mathrm{AG}(k,q)$ *which can be extended to an $(n+w)$-cap by some w points in the hyperplane at infinity, and*
- *An m-cap in* $\mathrm{PG}(l,q)$.

Then $\mathrm{PG}(k+l,q)$ *contains an $(nm+w)$-cap.*

An application to the elliptic quadric in $\mathrm{PG}(3,q)$ yields a classical construction of B. Segre [51]: an m-cap in $\mathrm{PG}(l,q)$ leads to an (q^2m+1)-cap in $\mathrm{PG}(l+3,q)$. A **tangent hyperplane** to a given point set in a projective space is a hyperplane which meets the point set in precisely one point. The following is [20, Theorem 10].

Theorem 4. *Assume the following exist:*

- *An n-cap in* $\mathrm{PG}(k,q)$ *possessing a tangent hyperplane, and*
- *An m-cap in* $\mathrm{PG}(l,q)$ *possessing a tangent hyperplane.*

Then $\mathrm{PG}(k+l,q)$ *contains an $(nm-1)$-cap.*

Application to the elliptic quadric in $\mathrm{PG}(3,q)$ yields a (q^4+2q^2)-cap in $\mathrm{PG}(6,q)$. For $q \geq 4$, this is the largest known cap in $\mathrm{PG}(6,q)$. This leads to the natural question if larger caps can be constructed in $\mathrm{PG}(6,q)$ for $q > 3$. Many of the best known caps, even in moderately small dimensions, have been constructed by applying some version of the product construction to caps from lower-dimensional spaces. Rather sophisticated product constructions are used in [17] to construct a 1216-cap in $\mathrm{PG}(9,3)$ (whose automorphism group is an extension of a normal subgroup of order 2^8 by S_5) and a 6464-cap in $\mathrm{PG}(11,3)$.

7 Families of caps in fixed dimension

We are interested in families of caps in $\mathrm{PG}(d,q)$ for all q, or at least for an infinite family of fields $\mathbb{F}_q$, whose number of points is $cq^\alpha +$ lower terms. What is the largest exponent α and, for this α, what is the largest constant c? We then speak of a family of order cq^α. Clearly $(\alpha,c) = (2,1)$ for $d = 3$.

The case of projective dimension $d = 4$

This is the smallest interesting dimension and it is difficult. It is not known if an exponent $\alpha > 2$ can be reached. Choosing elliptic quadrics in two solids shows that order $2q^2$ can always be reached. A family of order $2.5q^2$ for arbitrary odd characteristic is constructed in [9]. In characteristic 2, only one family of order cq^2 for $c > 2$ is known. This is a family of $(3q^2+4)$-caps $K_q \subset AG(4,q),\ q = 2^{odd}$ constructed in [23]. For $q = 2^{even}$ the existence of a family of caps of order cq^2, for $c > 2$, remains an open problem.

Definition 1. *Let $q = 2^f$. For $0 \neq v \in \mathbb{F}_q$, let p_v be the number of elements $0 \neq x \in \mathbb{F}_q$ such that*

$$tr(x) = tr(v/x) = 1$$

where $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_2$ is the absolute trace.

The elliptic curve with affine equation $y^2 + y = x + v/x$ has precisely $4p_v$ rational points. The weight distribution of the binary Kloosterman and Mélas codes are determined by the numbers p_v. Those numbers were determined by Schoof and van der Vlugt [48]. In [23], it is shown how the weight distribution of the cap-codes C_q corresponding to K_q is determined by the numbers p_v as well. In particular the minimum distance follows from the Hasse bound on the number of rational points of an elliptic curve. In the smallest case, C_8 is a $[196,5,164]_8$-code which can be extended to a $[200,5,168]_8$-code. This relation is one illustration of the use of algebraic geometry in coding theory. The most prominent such link is the construction of algebraic-geometric codes due to Goppa and Manin [34,40]. However there are many examples for the use of algebraic curves in determining the structure of classical codes as well.

The family K_q has more interesting structure. There is a special point P_0 such that $K_q \setminus \{P_0\}$ is a dual BCH-code, and those $3q+3$ points are distributed on three parabolic quadrics. This raises the general question to determine the cyclic codes of dual distance 4.

Projective dimension $d \leq 5$ over $\mathbb{F}_5$

A 66-cap in PG$(4,5)$ was found in [21] using a complicated recursive construction based on the ovoid in PG$(3,5)$. This 66-cap is rather symmetric. Its automorphism group is a direct product of A_5 and the dihedral group D_8. This indicates a rich geometric structure. In fact, the 66-cap in PG$(4,5)$ and its partner, a newly discovered 195-cap in PG$(5,5)$, turn out to be closely related to the conic section in PG$(2,5)$ and a classical geometric structure associated to it, the **Barlotti arcs** (see [2]). In the following we sketch the construction.

Start from the conic $C \subset PG(2,5)$ defined by the equation $Y^2 = XZ$. Its points are $P_\infty = (0:0:1)$ and $P_y = (1:y:y^2), y \in \mathbb{F}_5$. The tangents are

$$t_\infty = [1:0:0] \text{ and } t_y = [y^2 : -2y : 1].$$

These are the lines $[u:v:w]$, where $v^2 + uw = 0$. The interior points (those not on a tangent to C) are $(x:y:z)$, where $y^2 - xz$ is a non-square. These are the points $(1:y:z)$ where $y^2 - z = \pm 2$. The interior points are therefore $(1:y:y^2 \pm 2)$, where y is arbitrary. The secants are the lines $[u:v:w]$, where $v^2 + uw$ is a non-zero square and consequently the

exterior lines are $[u:v:w]$, where v^2+uw is a non-square. The exterior line $[-v^2+2:v:1]$ contains the interior points

$$(1:2v-1:-v^2+v+3),\ (1:2v+1:-v^2-v+3) \text{ and } (1:2v:-v^2+3).$$

The exterior line $[-v^2-2:v:1]$ contains the interior points

$$(1:2v-2:-v^2+2v+2),\ (1:2v+2:-v^2-2v+2) \text{ and } (1:2v:-v^2+2).$$

Definition 2. *A* **half-point** *is a pair $\pm v$ of non-zero vectors. The* **parity** *of a non-zero element of $\mathbb{F}_5$ is its quadratic remainder symbol.*

Observe that each point of $\mathrm{PG}(d,5)$ is the union of two half-points.

Definition 3. *Let $G \subset GL(3,5)$ the stabilizer of the set of vectors in $\mathbb{F}_5^3$ that represent the points of the conic C. Let*

$$K_\infty = (0,0,1) \text{ and } K_y = (1,y,y^2) \text{ for } y \in \mathbb{F}_5.$$

Define $K = \{\pm K_\tau \mid \tau \in PG(1,5)\}$, a system of half-points representing the points of C.

The group G acts on the two-element set $\{K, 2K\}$. The stabilizer of the system K of half-points is a subgroup $G_0 \subset G$ of index 2, where $G_0/\langle -1\rangle \cong S_5$ and $G/\langle -1\rangle \cong S_5 \times \mathbb{Z}_2$.

We turn to the action of G on vectors generating interior points.

Definition 4. *Let $I(y,1) = (1,y,y^2+2)$ and $I(y,2) = 2(1,y,y^2-2)$ for $y \in \mathbb{F}_5$. Then the union I of the $\pm I(y,1)$ and $\pm I(y,2)$ is a system of 10 half-points which generate the interior points of C.*

Here are those vectors:

$$(1,0,2),(1,1,3),(1,2,1),(1,3,1),(1,4,3)$$

$$(2,0,1),(2,1,4),(2,2,3),(2,3,3),(2,4,4).$$

Lemma 1. *The group G acts on the two-element set $\{I, 2I\}$. The stabilizer G_1 of the system I of half-points representing interior points satisfies $G_1/\langle -1\rangle \cong S_5$.*

The points $(1:I)$ form a 20-cap in $\mathrm{AG}(3,5)$. The stabilizer G_2 of K and I in G satisfies $G_2/\langle -1\rangle \cong A_5$. Most important is the following lemma:

Lemma 2. *The half-points in $K \cup I$ have the following property: Let K_1, K_2, I_1, I_2 be non-zero vectors in $\mathbb{F}_5^3$ such that K_1, K_2 belong to different half-points from K and I_1, I_2 belong to different half-points from I.*

- *If $c_1K_1 + c_2K_2 + dI_1 = 0$, where $c_1, c_2, d \in \mathbb{F}_5$, not all $= 0$, then c_1, c_2 are non-zero of different parity.*
- *If $cK_1 + d_1I_1 + d_2I_2 = 0$, where $c, d_1, d_2 \in \mathbb{F}_5$, not all $= 0$, then d_1, d_2 are non-zero of different parity.*

This leads to a recursive construction procedure:

Theorem 5. *Let $l \geq 2$ and $A, B \subset \mathbb{F}_5^l$ such that the following are satisfied:*

1. *$0 \notin A = -A, 0 \notin B = -B$. In other words, A is the union of $|A|/2$ half-points, likewise for B. Denote by C_A, C_B the corresponding point sets in* $\mathrm{PG}(l-1,5)$.
2. *The set C_B is a $|B|/2$-cap in* $\mathrm{PG}(l-1,5)$.
3. *The points $(1:a), a \in A$, form a cap in* $\mathrm{AG}(l,5)$ *(equivalently: $(A+A) \cap 2A = \emptyset$).*
4. *$C_A \cap C_B = \emptyset$.*
5. *The points represented by $A + 2A$ are disjoint from the points represented by B, and symmetrically with the roles of A, B exchanged.*

Then the points (P,a) and (Q,b) where $P \in K, Q \in I$ and $a \in A, b \in B$ represent a cap M of size $6|A| + 10|B|$ in $\mathrm{PG}(l+2,5)$.

In case $l = 2$, let

$$A = \pm\{(1,0),(1,2)\},\ B = \pm\{(0,1),(1,1)\}.$$

Then the conditions of Theorem 5 are satisfied. It follows that M is a 64-cap in $\mathrm{PG}(4,5)$. Points $(0:0:0:1:3)$ and $(0:0:0:1:4)$ are extension points. This yields a 66-cap. Each of the extension points is on an obvious tangent hyperplane. At this point, we have reconstructed the 66-cap in $\mathrm{PG}(4,5)$. A similar process works one dimension higher.

Let $l = 3$. Choose $A = K$ the union of the representatives of conic half-points. It is possible to find B with the same structure as K for a conic disjoint from C. One choice is the quadric $Q(X,Y,Z) = X^2 + Z^2 - 2(XY + XZ + YZ)$ and its half-points

$$B = \pm\{010, 101, 012, 210, 112, 211\}.$$

This yields a 192-cap in $\mathrm{PG}(5,5)$ by Theorem 5. Observe that B consists entirely of exterior points with respect to A. There are three extension points yielding a 195-cap in $\mathrm{PG}(5,5)$.

Higher dimensions

In characteristic 2, the product construction applied to hyperovals and elliptic quadrics yields $(q+2)(q^2+1)$-caps in $\mathrm{PG}(5,q)$. Recently, Kroll-Vincenti [39] constructed $\big((q+2)(q^2+2)-1\big)$-caps in $\mathrm{PG}(5,q)$ for even $q \geq 8$. In odd characteristic a rather specialized version of the product construction (see [20]) applied to elliptic quadrics and conic sections yields $(q+1)(q^2+3)$-caps in $\mathrm{PG}(5,q)$. The (q^4+2q^2)-caps in $\mathrm{PG}(6,q)$ for arbitrary q have been mentioned before as an application of Theorem 4. An application of Theorem 3 to this cap produces $q^2(q^2+1)^2$-caps in $\mathrm{PG}(9,q)$.

8 Concrete bounds

Here is a list of the currently best known lower bounds on large caps in $\mathrm{PG}(d,q)$, for $d \leq 11$ and $q \leq 9$. The superscript c indicates that the cap is known to be complete.

The lower bounds are known to agree with the upper bound only when $d \leq 3$, for $d \leq 5$ in the ternary and for $d = 4$ in the quaternary case. The upper bound in $\mathrm{PG}(6,3)$ currently is 136 [1]. In $\mathrm{PG}(4,5)$ the upper bound is 88 [26].

$d\backslash q$	3	4	5	7	8	9
2	4^c	6^c	6^c	8^c	10^c	10^c
3	10^c	17^c	26^c	50^c	65^c	82^c
4	20^c	41^c	66^c	132^c	208^c	212^c
5	56^c	126^c	195^c	434^c	695^c	840^c
6	112^c	288^c	675^c	2499^c	4224^c	6723^c
7	248^c	756^c	1715^c	6472^c	13520^c	17220^c
8	541^c	2110^c	5069^c	21555^c	45174	68070
9	1216^c	5040^c	17124^c	122500	270400	544644
10	2744^c	15423^c	43876	323318	878800	1411830
11	6464^c	34566	130951	1067080	2931457	5580100

Table 1: Lower bounds

9 The atoms of cap theory

Most of the known large caps in larger dimensions result from applications of some recursive construction to exceptionally large caps in lower dimensions. This raises the question what the elementary building blocks are, the large caps which do not result from recursive constructions themselves and which are used as ingredients for the constructions in higher dimensions. We call them the atoms of cap theory. Clearly, the classical models have that status, see Section 2. Also large caps possessing a large group of automorphisms will be considered to be atoms. This leads to the following list of atoms:

1. The ovals and hyperovals in $\mathrm{AG}(2,q)$.
2. The elliptic quadrics in $\mathrm{PG}(3,q)$.
3. The Tits ovoids in $\mathrm{PG}(3,2^{2m+1}), m \geq 1$.
4. The Hill cap in $\mathrm{PG}(5,3)$.
5. The highly symmetric 41-cap in $\mathrm{PG}(4,4)$ and its dual partner, the 40-cap in $\mathrm{AG}(4,4)$.
6. The Glynn cap in $\mathrm{PG}(5,4)$.

Now we present some more examples of caps that have the potential to be regarded as atoms.

The complete 14-cap in $\mathrm{PG}(3,4)$

This object is uniquely determined. Its group of automorphisms is the semidirect product of an elementary abelian group of order 8 and $\mathrm{GL}(3,2)$ (see [19]). Here is a construction using only hyperovals: there is a configuration in $\mathrm{PG}(3,4)$ consisting of three collinear planes and a hyperoval in each plane, where the line of intersection is a secant for all three hyperovals. The union of those hyperovals is our 14-cap. We will encounter it in

Section 11 as a quantum cap. It is also used in the construction of a quantum 38-cap in PG$(4,4)$. The complete 14-cap in PG$(3,4)$ is a special case of a result of Segre [52] who constructed complete $(3q+2)$-caps in PG$(3,q)$ for all even $q \geq 4$. The construction was further generalized by Pambianco-Storme [44].

A 66-cap in PG$(4,5)$

It has been mentioned in Section 7 that its group of automorphisms is $A_5 \times D_8$. It possesses a tangent hyperplane and therefore can be used in Theorem 4. This produces a 1715-cap in PG$(7,5)$.

A 132-cap in PG$(4,7)$

This cap resulted from a computer search. Its automorphism group has order 192.

A 208-cap in PG$(4,8)$

This is the largest cap known in PG$(4,8)$. It resulted from a computer construction based on a cyclic group of order $8^2-1=63$. We raise the problem if this construction can be generalized in the following way: a $(3q^2+2q)$-cap in PG$(4,q)$, $q=2^{2m+1}$, admitting the action of a certain cyclic group of order q^2-1, consisting of 3 regular orbits, one orbit of length $q+1$, one orbit of length $q-1$, and three fixed points. The conjecture is true for $q=8$ and for $q=32$.

A 195-cap in PG$(5,5)$

This cap was constructed as an application of Theorem 5. It possesses tangent hyperplanes and therefore can be used in Theorem 4. With the elliptic quadric in PG$(3,5)$ as second ingredient, this yields a 5069-cap in PG$(8,5)$. Application of Theorem 3 to the 195-cap in in PG$(5,5)$ and the 675-cap in PG$(6,5)$ yields a cap with $194 \times 675 + 1 = 130,951$ points in PG$(11,5)$. We saw in an earlier subsection that the 66-cap in PG$(4,5)$ and the 195-cap in PG$(5,5)$ result from a recursive construction which only uses a conic and its embedding in the plane as ingredients. It is therefore up to discussion if those caps should be considered as atoms. The automorphism group of the 195-cap is isomorphic to $A_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2$.

A 434-cap in PG$(5,7)$

The Glynn cap makes use of a certain mapping $\gamma : PG(2,q^2) \longrightarrow PG(5,q)$. The image Γ_q of this mapping is a set of $(q^4-q)/2$ points. In case $q=4$, this is the Glynn cap. In [21], a computer program produced a subset of $\Gamma_7 \subset PG(5,7)$, which is a 434-cap whose automorphism group has order $672 = 4 \times 168$. This automorphism group is not solvable. It involves the simple group of order 168. It may be possible to find further large caps as subsets of Γ_q. If synthetic constructions can be found, it may be the case that the Glynn cap is the beginning of an infinite family of caps in PG$(5,q)$.

Most of the automorphism groups were calculated using Thomas Feulner's program [29] which is available online, see also the paper [28].

10 An asymptotic problem

As in Section 5, let $C_k(q)$ be the maximum size of a cap in $\mathrm{AG}(k,q)$. Define

$$\mu(q) = \lim_{k \longrightarrow \infty} \sup \log_q(C_k(q))/k.$$

Clearly, we could use caps in $\mathrm{PG}(k,q)$ instead of $\mathrm{AG}(k,q)$ and obtain the same limit. Working with affine caps has the advantage that because of the product construction of Theorem 2, each value $C_k(q)$ in a concrete dimension k yields a lower bound: $\mu(q) \geq \log_q(C_k(q))/k$. In particular, the affine part of the elliptic quadric in $\mathrm{PG}(3,q)$ yields $\mu(q) \geq 2/3$. A basic open problem is to show that $\mu(q) < 1$. The best known lower bound for general q seems to follow from an application of Theorem 4 to elliptic quadrics, see [20]. This leads to a cap of size $(q^2+1)^2 - 1 = q^4 + 2q^2$ in $\mathrm{PG}(6,q)$. It is easy to see that there is a hyperplane meeting this cap in q^2+1 points. This leads to an (q^4+q^2-1)-cap in $\mathrm{AG}(6,q)$ and the lower bound $\mu(q) \geq \log_q(q^4+q^2-1)/6$. For $q=4$, the affine part of the Glynn-cap yields a better lower bound: $\mu(4) \geq \log_4(120)/5 = 0,6906\ldots$ As is to be expected, the ternary case has been studied most intensively. The recursive constructions of Calderbank-Fishburn [14] based on the Hill cap have been further refined in [17]. Currently, the best known lower bound is $\mu(3) \geq 0,724851\ldots$

11 Additive codes and quantum caps

Additive codes are a far-reaching generalization of linear codes. Here we view the alphabet of size q^m not as a field but rather as a vector space over the subfield $\mathbb{F}_q$ and assume linearity only over $\mathbb{F}_q$. Of particular interest is the quaternary case ($q = m = 2$).

Definition 5. *Let k be such that $2k$ is a positive integer. An additive quaternary $[n,k]_4$-code C (length n, dimension k) is a $2k$-dimensional subspace of $\mathbb{F}_2^{2n}$, where the coordinates come in pairs of two. We view the codewords as n-tuples where the coordinate entries are elements of $\mathbb{F}_2^2$.*

A **generator matrix** *of C is a binary $(2k,2n)$-matrix whose rows form a basis of the binary vector space C.*

One reason to concentrate on the quaternary case is the link with quantum error-correction established in [15]. It may be described equivalently using the symplectic form, which is a basic notion from geometric algebra.

Definition 6. *Let $V = V(2n,q)$ be a $2n$-dimensional vector space over $\mathbb{F}_q$. A* **symplectic form** *on V is a mapping $\langle , \rangle : V \oplus V \longrightarrow \mathbb{F}_q$ which satisfies the following conditions:*

- $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$, $\langle x, y_1 + y_2\rangle = \langle x, y_1\rangle + \langle x, y_2\rangle$ *and* $\langle cx, y\rangle = \langle x, cy\rangle = c\langle x, y\rangle$ *for all $x, x_i, y, y_i \in V, c \in \mathbb{F}_q$.*
- $\langle x, x\rangle = 0$ *for all $x \in V$.*

- *The only vector x satisfying $\langle x,y\rangle = 0$ for all $y \in V$ is $x = 0$.*

If $\langle x,y\rangle = 0$ we also write $x \perp y$ and $y \in x^{\perp}$. Let $W \subset V$. The dual of W is a subspace defined by

$$W^{\perp} = \{y | y \in V, \langle w,y\rangle = 0 \text{ for all } w \in W\}.$$

A symplectic space V possesses a **symplectic basis** $\{v_1,\ldots,v_n,w_1,\ldots,w_n\}$ such that $\langle v_i,v_j\rangle = \langle w_i,w_j\rangle = 0$ for all i,j and $\langle v_i,w_j\rangle = \delta_{i,j}$.
The pertinent notion is the following.

Definition 7. *A pure additive quantum stabilizer $[[n,m,d]]$-code C (short: quantum code) is a quaternary additive code C of length n and dimension $(n-m)/2$ which satisfies*

- *$C \subseteq C^{\perp}$ where the dual is with respect to the symplectic form.*
- *$C^{\perp}$ has distance $\geq d$.*

The translation into geometry is as follows, see [11]:

Theorem 6. *The following are equivalent:*

- *A pure $[[n,n-r,t+1]]$ quantum stabilizer code.*
- *A set of n lines, the* **codelines***, in $\mathrm{PG}(r-1,2)$ satisfying:*
  - *any t codelines are in general position and*
  - *the quantum condition: for every secundum (subspace $\mathrm{PG}(r-3,2)$) S, the number of codelines skew to S is even.*

In particular, pure quantum codes are always described in terms of sets of pairwise skew lines in binary projective space. When $d = 3$, the only additional condition to satisfy is the quantum condition. In contrast to the classical theory of linear codes, even case $d = 3$ is not trivial. The classification of all parameters n,m such that $[[n,m,3]]$ quantum codes exist is very recent, see [8].
The smallest open case is $d = 4$ and the corresponding quantum codes form a natural generalization of the concept of a cap. Under the additional hypothesis that the code be not only additive, but also $\mathbb{F}_4$-linear, the concept of a quantum cap is obtained:

Definition 8. *A* **pre-quantum cap** *is an n-cap $K \subset PG(m-1,4)$ which satisfies the following equivalent conditions:*

- *$K \cap H$ has the same parity as n for every hyperplane H.*
- *The corresponding quaternary linear cap-code $C(K)$ has all weights even.*
- *$C(K)$ is self-orthogonal with respect to the Hermitian form.*

A **quantum cap** *in $\mathrm{PG}(m-1,4)$ is a pre-quantum cap which is not contained in a proper subspace.*

Here the Hermitian form on $\mathbb{F}_4^m$ is defined by $B((x_1,x_2,\ldots,x_m),(y_1,y_2,\ldots,y_m)) = \sum_{i=1}^m x_i y_i^2$. A quantum n-cap in $\mathrm{PG}(m-1,4)$ is equivalent to a pure $[[n,n-2m,4]]$ quantum code which is $\mathbb{F}_4$-linear. As an example, consider the elliptic quadric in $\mathrm{PG}(3,4)$. As this cap has 17 points and plane intersections of sizes 1 or 5, the conditions of Definition 8 are satisfied. The corresponding cap-code is a $[17,4,12]_4$-code and it is a $[[17,9,4]]$ quantum code. The smallest quantum cap in $\mathrm{PG}(3,4)$ has 8 points. It may be constructed as the complement of $\mathrm{PG}(2,2)$ in $\mathrm{PG}(3,2)$, where $\mathrm{PG}(3,2)$ is embedded in $\mathrm{PG}(3,4)$. This is a quantum $[[8,0,4]]$-code. The cardinalities of quantum caps in $\mathrm{PG}(3,4)$ are $8,12,14,17$. The cardinalities of quantum caps in $\mathrm{PG}(4,4)$ are a priori between 10 (the obvious theoretical minimum) and 41, the size of the largest cap in $\mathrm{PG}(4,4)$. In fact, one of the two 41-caps in $\mathrm{PG}(4,4)$ is quantum as is the uniquely determined largest cap in $\mathrm{AG}(4,4)$, which has 40 points. Here is a construction of a quantum 10-cap in $\mathrm{PG}(4,4)$: choose two planes Π_1,Π_2 in $\mathrm{PG}(4,4)$ which intersect in a point P. Choose ovals $O_i \subset \Pi_i$ such that P is the nucleus of O_i. Then $O_1 \cup O_2$ is a quantum cap. The most obvious recursive construction is the following

Theorem 7. *Let K_1,K_2 be disjoint pre-quantum caps in $\mathrm{PG}(m-1,4)$. If $K_1 \cup K_2$ is a cap, then it is a pre-quantum cap.*

Let $K_1 \subset K_2$ be pre-quantum caps. Then also $K_2 \setminus K_1$ is a pre-quantum cap.

This theorem can be used in two ways. One is to start from a quantum cap K_2 and construct quantum caps $K_1 \subset K_2$. This point of view was adopted by Tonchev [56] who found quantum caps contained in the quantum 41-cap in $\mathrm{PG}(4,4)$ (of sizes $n \in \{10,12,14-27,29,31,33,35\}$) and in the Glynn cap, a 126-cap in $\mathrm{PG}(5,4)$ which is quantum. The question which subcaps of a given quantum cap are pre-quantum can be expressed in terms of a certain binary code.

Definition 9. *Let K be a cap in $\mathrm{PG}(m-1,4)$ and M a corresponding generator matrix. The* **associated binary code** *A is the binary linear code of length n generated by the supports of the quaternary codewords of the code generated by M.*

Observe that by definition, K is pre-quantum if and only if A is contained in the all-even code. This leads to the following characterization.

Theorem 8. *Let $K \subset PG(m-1,4)$ be pre-quantum and $K_1 \subseteq K$. Then K_1 (and its complement $K \setminus K_1$) is pre-quantum if and only if the characteristic vector of K_1 is contained in the dual $A^\perp$ of the binary code A associated to K.*

This is essentially Theorem 7 of [15].

The other way how to use Theorem 7 is to construct quantum caps as a union $K_1 \cup K_2$ of two disjoint pre-quantum caps K_1 and K_2. This often leads to more transparent constructions. For example, a quantum 12-cap in $\mathrm{PG}(3,4)$ can be constructed simply as the union of two disjoint hyperovals on two planes. Bartoli [3] describes a quantum 20-cap in $\mathrm{PG}(4,4)$ and constructs more quantum caps in $\mathrm{PG}(4,4)$ of cardinalities $29,30,32,33,34$ in [5]. Theorem 7 can be generalized.

Theorem 9. *Let Π_1,Π_2 be different hyperplanes of $\mathrm{PG}(m,4)$ and $K_i \subset \Pi_i$ be pre-quantum caps such that $K_1 \cap \Pi_1 \cap \Pi_2 = K_2 \cap \Pi_1 \cap \Pi_2$. Then the symmetric sum $K_1 + K_2 = (K_1 \setminus K_2) \cup (K_2 \setminus K_1)$ is a pre-quantum cap.*

Theorem 10. *Let Π_1, Π_2 be different $(m-2)$-dimensional subspaces of $\mathrm{PG}(m,4)$ which together generate $\mathrm{PG}(m,4)$. Let $K_i \subset \Pi_i$ be pre-quantum caps such that $K_1 \cap \Pi_1 \cap \Pi_2 = K_2 \cap \Pi_1 \cap \Pi_2$. Then the symmetric sum $K_1 + K_2$ is a pre-quantum cap.*

As an application of Theorem 10, choose two planes Π_1, Π_2 in $\mathrm{PG}(4,4)$ which meet in a point X. Let $K_i \cup \{X\}$ be a hyperoval in Π_i, for $i = 1,2$. Then the symmetric sum $K_1 \cup K_2$ is a quantum 10-cap in $\mathrm{PG}(4,4)$. In [4], we give geometric constructions of quantum 36-caps and of quantum 38-caps in $\mathrm{PG}(4,4)$. This yields new quantum codes with parameters $[[36,26,4]]$ and $[[38,28,4]]$.

Tonchev [56] found a quantum 27-cap in $\mathrm{PG}(6,4)$ by the action of an automorphism of order 13. It turns out that the dual distance is in fact 5, so this yields a quaternary linear $[[27,13,5]]$-quantum code.

In [11], a quantum 5040-cap in $\mathrm{PG}(9,4)$ and a quantum 756-cap in $\mathrm{PG}(7,4)$ are constructed. For a long time, the smallest open problem on additive quantum codes concerned the existence of $[[13,5,4]]$-quantum codes. This has been settled in [12]: such a quantum code does not exist.

12 A problem in additive number theory

Definition 10. *Let A be an abelian group, written additively, and $e = exp(A)$ its exponent, i.e. the lowest common multiple of its element orders. A* **sequence** *over A is a mapping $\sigma : A \longrightarrow \{0,1,2,\dots\}$. We think of a sequence as a multiset, where each element $a \in A$ occurs with multiplicity $\sigma(a)$. The size of a sequence is $\sum_a \sigma(a)$.*
A sequence $S(A)$ is a sequence over A which does not contain subsequences of size e which sum to 0. Denote by $l(A)$ the largest size of a sequence $S(A)$.

The problem is the determination of $l(A)$. This problem and certain related problems have a long history in additive number theory. Clearly, all multiplicities of elements in a sequence $S(A)$ are bounded by $e-1$.

In the literature mostly the case of homocyclic groups $A = \mathbb{Z}_m^n$ is considered. One reason for this may have been the following observation: $l(\mathbb{Z}_m^n)+1$ is the smallest number N such that each set of N points in the rank n integer lattice $\mathbb{Z}^n$ contains a subset of m points whose centroid is in $\mathbb{Z}^n$. Clearly $exp(\mathbb{Z}_m^n) = exp(\mathbb{Z}_m) = m$. In case $m = 3$, there is an obvious link to affine caps. Recall from Section 5 that $C_n(q)$ denotes the largest size of a cap in $\mathrm{AG}(n,q)$.

Proposition 1. $l(\mathbb{Z}_3^n) = 2C_n(3)$.

Proof. This follows directly from the fact that a subset of $\mathrm{AG}(n,3)$ is a cap if and only if it does not contain a 3-subset summing to 0. If K is a cap, then the multiset $2K$, where each element of K appears with multiplicity 2, is a sequence $S(\mathbb{Z}_3^n)$. On the other hand, if a sequence $S(\mathbb{Z}_3^n)$ is given, then using each element of multiplicity > 0 with multiplicity 2 produces a sequence $S(\mathbb{Z}_3^n)$ which has the form $2K$, where K is a cap. □

Recall that each abelian group can be written as a direct product $A = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ where $m_1 \mid \cdots \mid m_r$ in a unique way and r is the **rank** of A, the largest rank of its Sylow p-subgroups, where p varies over the prime divisors of $|A|$. For rank ≤ 2, the answer to our problem is known:

Theorem 11. *Let $A = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ where $m_1 \mid m_2$. Then $l(A) = 2m_1 + 2m_2 - 4$.*

A proof is in [32]. For rank one, this implies $l(\mathbb{Z}_m) = 2m-2$. This implies that each sequence of $2m-1$ integers contains a subsequence of m integers which sum to 0 mod m. This is the Erdös-Ginzburg-Ziv theorem, see Section 2.4 of Nathanson [43].

A global approach

Here is a related global problem.

Definition 11. *A subset $U \subset \{0,1,2,\dots\}^n$ is a sequence $S(n,\mathbb{Z})$ if for each odd integer m, the multiset $(m-1)(U \bmod m)$ is a sequence $S(\mathbb{Z}_m^n)$.*

Here $(m-1)(U \bmod m)$ stands for the following: each element of U is read mod m in each component, the resulting tuple in $\mathbb{Z}_m^n$ is used with multiplicity $m-1$. In particular each sequence $S(n,\mathbb{Z})$ of cardinality u yields a sequence $S(\mathbb{Z}_m^n)$ of cardinality $(m-1)u$, for each odd m. Choosing $m=3$, we see that U mod 3 is a cap in $\mathrm{AG}(n,3)$, consequently $|U| \le C_n(3)$.

Proposition 2. *Let $U = \{0,1\}^n$. Then S is a sequence $S(n,\mathbb{Z})$ of size 2^n.*

Proof. Assume S is a multisubset of $(m-1)(U \bmod m)$, defined by multiplicities $\mu_v \le m-1$ for $v \in S$, such that $\sum \mu_v = m$ and $\sum \mu_v v \equiv 0 \pmod m$. The coordinate entries in $\sum \mu_v v$ are 0 or m. Let $v \neq v'$ such that $\mu_v > 0, \mu_{v'} > 0$. Choose notations such that there exists a coordinate i with $v_i = 0, v'_i = 1$. Then coordinate i yields a contradiction. There is therefore only one v such that $\mu_v > 0$. This yields the contradiction $\mu_v = m$. □

Proposition 2 is due to Harborth [35]. This result implies $l(\mathbb{Z}_m^n) \ge (m-1)2^n$. Sets $S(3,\mathbb{Z})$ and $S(4,\mathbb{Z})$ of maximal sizes $C_3(3) = 9$ and $C_4(3) = 20$, respectively, were constructed in [24, 27]. Here is the sequence $S(3,\mathbb{Z})$ of size 9 as given in [27]. It is in fact contained in $\{0,1,2\}^3$ and consists of the following triples:

$$(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,0,1),(0,1,1),(1,1,2),(1,2,2),(2,1,2).$$

Let us check the defining property for $m=3$. This is equivalent with the statement that the set of points $(1 : x_2 : x_3 : x_4) \in AG(3,3)$, where $x = (x_2,x_3,x_4)$ varies over the nine triples above and entries are interpreted in $\mathbb{Z}/3\mathbb{Z}$, form a cap. In fact all those points are on the quadric $x_2^2 + x_3^2 + x_4^2 - x_1x_2 - x_1x_3 - x_1x_4 + x_2x_3 = 0$. This is an elliptic quadric in $\mathrm{PG}(3,3)$ whose points therefore form a cap. As a consequence $l(\mathbb{Z}_m^3) \ge 9(m-1)$ for all odd $m \ge 3$. It is conjectured in Gao-Thangadurai [31] that equality always holds. The conjecture has been confirmed for $m = 3^a 5^b$, see [30]. An analogous conjecture concerning $\mathbb{Z}_m^4$ is made in [24]: $l(\mathbb{Z}_m^4) = 20(m-1)$ for all odd $m \ge 3$.

In [18], a product construction is used to produce sequences $S(5,\mathbb{Z}), S(6,\mathbb{Z}), S(7,\mathbb{Z})$ of sizes 42, 96, and 192, respectively. As 42 is the size of the second-largest complete cap in $\mathrm{AG}(5,3)$ (this fact is proved in [18]), it follows that any sequence $S(5,\mathbb{Z})$ of size > 42 must have the property that its image mod 3 is contained in the affine Hill cap. The existence of such a sequence $S(5,\mathbb{Z})$ remains an open problem. Another open problem concerns the following conjecture: Each sequence $S(A)$ of maximal length $l(A)$ arises from a subset of A by using each element with multiplicity $e-1$.

References

[1] J. BARÁT, Y. EDEL, R. HILL, AND L. STORME, *On complete caps in the projective geometries over* $\mathbb{F}_3$. *II. New improvements*, J. Combin. Math. Combin. Comput., 49 (2004), pp. 9–31.

[2] A. BARLOTTI, *Some topics in finite geometrical structures*, Tech. Rep. 439, Institute of Statistics, University of Carolina, Mimeo Series, 1965.

[3] D. BARTOLI, *Quantum codes and related geometric properties*, PhD thesis, University of Perugia, 2008.

[4] D. BARTOLI, J. BIERBRAUER, S. MARCUGINI, AND F. PAMBIANCO, *Geometric constructions of quantum codes*, in Proceedings of the Conference on Error-Correcting Codes, Cryptography and Finite Geometries, A. A. Bruen and D. L. Wehlau, eds., to appear.

[5] D. BARTOLI, S. MARCUGINI, AND F. PAMBIANCO, *New quantum caps in* $PG(4,4)$. manuscript.

[6] J. BIERBRAUER, *Large caps*, J. Geom., 76 (2003), pp. 16–51. Combinatorics, 2002 (Maratea).

[7] ——, *Introduction to coding theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.

[8] ——, *The spectrum of stabilizer quantum codes of distance* 3, IEEE Trans. Inform. Theory, submitted, (2010).

[9] J. BIERBRAUER AND Y. EDEL, *A family of caps in projective* 4*-space in odd characteristic*, Finite Fields Appl., 6 (2000), pp. 283–293.

[10] ——, *Bounds on affine caps*, J. Combin. Des., 10 (2002), pp. 111–115.

[11] J. BIERBRAUER, G. FAINA, M. GIULIETTI, S. MARCUGINI, AND F. PAMBIANCO, *The geometry of quantum codes*, Innov. Incidence Geom., 6/7 (2007/08), pp. 53–71.

[12] J. BIERBRAUER, S. MARCUGINI, AND F. PAMBIANCO, *The non-existence of a* $[[13,5,4]]$ *quantum stabilizer code*, `http://arxiv.org/abs/0908.1348v1`, (2009).

[13] R. C. BOSE, *Mathematical theory of the symmetrical factorial design*, Sankhyā, 8 (1947), pp. 107–166.

[14] R. CALDERBANK AND P. C. FISHBURN, *Maximal three-independent subsets of* $\{0,1,2\}^n$, Des. Codes Cryptogr., 4 (1994), pp. 203–211.

[15] R. CALDERBANK, E. M. RAINS, P. W. SHOR, AND N. J. A. SLOANE, *Quantum error correction via codes over* GF(4), IEEE Trans. Inform. Theory, 44 (1998), pp. 1369–1387.

[16] B. L. DAVIS AND D. MACLAGAN, *The card game SET*, Math. Intelligencer, 25 (2003), pp. 33–40.

[17] Y. EDEL, *Extensions of generalized product caps*, Des. Codes Cryptogr., 31 (2004), pp. 5–14.

[18] ——, *Sequences in abelian groups G of odd order without zero-sum subsequences of length* $\exp(G)$, Des. Codes Cryptogr., 47 (2008), pp. 125–134.

[19] Y. EDEL AND J. BIERBRAUER, 41 *is the largest size of a cap in* $\mathrm{PG}(4,4)$, Des. Codes Cryptogr., 16 (1999), pp. 151–160.

[20] ——, *Recursive constructions for large caps*, Bull. Belg. Math. Soc. Simon Stevin, 6 (1999), pp. 249–258.

[21] ——, *Large caps in small spaces*, Des. Codes Cryptogr., 23 (2001), pp. 197–212.

[22] ——, *The largest cap in* $\mathrm{AG}(4,4)$ *and its uniqueness*, Des. Codes Cryptogr., 29 (2003), pp. 99–104.

[23] ——, *Caps of order* $3q^2$ *in affine 4-space in characteristic 2*, Finite Fields Appl., 10 (2004), pp. 168–182.

[24] Y. EDEL, C. ELSHOLTZ, A. GEROLDINGER, S. KUBERTIN, AND L. RACKHAM, *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math., 58 (2007), pp. 159–186.

[25] Y. EDEL, S. FERRET, I. LANDJEV, AND L. STORME, *The classification of the largest caps in* $\mathrm{AG}(5,3)$, J. Combin. Theory Ser. A, 99 (2002), pp. 95–110.

[26] Y. EDEL, L. STORME, AND P. SZIKLAI, *New upper bounds on the sizes of caps in* $\mathrm{PG}(N,5)$ *and* $\mathrm{PG}(N,7)$, J. Combin. Math. Combin. Comput., 60 (2007), pp. 7–32.

[27] C. ELSHOLTZ, *Lower bounds for multidimensional zero sums*, Combinatorica, 24 (2004), pp. 351–358.

[28] T. FEULNER, *The automorphism groups of linear codes and canonic representatives of their semilinear isometry classes*, Adv. Math. Commun., 3 (2009), pp. 363–383.

[29] ——. `http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/CanonicalForm/index.html`, 2010.

[30] W. D. GAO, Q. H. HOU, W. A. SCHMID, AND R. THANGADURAI, *On short zero-sum subsequences. II*, Integers, 7 (2007), pp. A21, 22 pp. (electronic).

[31] W. D. GAO AND R. THANGADURAI, *On zero-sum sequences of prescribed length*, Aequationes Math., 72 (2006), pp. 201–212.

[32] A. GEROLDINGER AND F. HALTER-KOCH, *Non-unique factorizations*, vol. 278 of Pure and Applied Mathematics (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[33] D. G. GLYNN, *A* 126*-cap of* PG$(5,4)$ *and its corresponding* $[126,6,88]$*-code*, Util. Math., 55 (1999), pp. 201–210.

[34] V. D. GOPPA, *Codes and information*, Uspekhi Mat. Nauk, 39 (1984), pp. 77–120.

[35] H. HARBORTH, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math., 262/263 (1973), pp. 356–360. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday.

[36] R. HILL, *On the largest size of cap in* $S_{5,3}$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8), 54 (1973), pp. 378–384 (1974).

[37] ——, *Caps and groups*, in Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo II, Accad. Naz. Lincei, Rome, 1976, pp. 389–394. Atti dei Convegni Lincei, No. 17.

[38] J. W. P. HIRSCHFELD AND L. STORME, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, in Finite geometries, vol. 3 of Dev. Math., Kluwer Acad. Publ., Dordrecht, 2001, pp. 201–246.

[39] H.-J. KROLL AND R. VINCENTI, *Antiblocking systems and PD-sets*, Discrete Math., 308 (2008), pp. 401–407.

[40] Y. I. MANIN, *What is the maximum number of points on a curve over* $\mathbf{F}_2$*?*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28 (1981), pp. 715–720 (1982).

[41] R. MESHULAM, *On subsets of finite abelian groups with no* 3*-term arithmetic progressions*, J. Combin. Theory Ser. A, 71 (1995), pp. 168–172.

[42] A. C. MUKHOPADHYAY, *Lower bounds on* $m_t(r,s)$, J. Combinatorial Theory Ser. A, 25 (1978), pp. 1–13.

[43] M. B. NATHANSON, *Additive number theory*, vol. 165 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[44] F. PAMBIANCO AND L. STORME, *Small complete caps in spaces of even characteristic*, J. Combin. Theory Ser. A, 75 (1996), pp. 70–84.

[45] G. PELLEGRINO, *Sul massimo ordine delle calotte in* $S_{4,3}$, Matematiche (Catania), 25 (1970), pp. 149–157 (1971).

[46] A. POTECHIN, *Maximal caps in* AG$(6,3)$, Des. Codes Cryptogr., 46 (2008), pp. 243–259.

[47] B. QVIST, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys., 1952 (1952), p. 27.

[48] R. SCHOOF AND M. VAN DER VLUGT, *Hecke operators and the weight distributions of certain codes*, J. Combin. Theory Ser. A, 57 (1991), pp. 163–186.

[49] B. SEGRE, *Sulle ovali nei piani lineari finiti*, Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat. (8), 17 (1954), pp. 141–142.

[50] ——, *Ovals in a finite projective plane*, Canad. J. Math., 7 (1955), pp. 414–416.

[51] ——, *Le geometrie di Galois*, Ann. Mat. Pura Appl. (4), 48 (1959), pp. 1–96.

[52] ——, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, Acta Arith., 5 (1959), pp. 315–332 (1959).

[53] L. STORME, J. A. THAS, AND S. K. J. VEREECKE, *New upper bounds for the sizes of caps in finite projective spaces*, J. Geom., 73 (2002), pp. 176–193.

[54] G. TALLINI, *Calotte complete di $S_{4,q}$ contenenti due quadriche ellittiche quali sezioni iperpiane*, Rend. Mat. e Appl. (5), 23 (1964), pp. 108–123.

[55] J. TITS, *Ovoïdes et groupes de Suzuki*, Arch. Math., 13 (1962), pp. 187–198.

[56] V. TONCHEV, *Quantum codes from caps*, Discrete Math., 308 (2008), pp. 6368–6372.